In the Claims

Claims 1, 8, 11, 13, 20, 23-25, 28 30, and 32 are currently amended.

Claim 2 is canceled herein.

Claims 1, 3, 6-13, 16-20, 23-25, 27-28, and 30-33 are pending and are listed below.

1. (Currently Amended) A processor-readable medium having a tangible component and comprising processor-executable instructions configured for:

receiving a binary signature at a server computing device, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file located on a client computing device;

receiving a security patch at the server computing device;

identifying, from the server computing device, [[a]] the particular vulnerable binary file located on [[a]] the client computing device based on the binary signature, the client computing device being remote from the server computing device; [[and]]

updating, from the server computing device, the particular vulnerable binary file located on the client computing device with the security patch[[.]]; and

wherein the identifying of the particular vulnerable binary file located on a client computing device comprises comparing the bit pattern that is associated with the security vulnerability in the particular vulnerable binary file against bit patterns of binary files located on the client computing device, and wherein the updating of the particular vulnerable binary file occurs if a bit pattern of the

particular vulnerable binary file exactly matches the bit pattern of the binary signature that is associated with the security vulnerability.

2. (Canceled)

3. (Previously Presented) A processor-readable medium as recited in claim 1, wherein the updating the vulnerable binary file located on the client computing device includes installing the security patch on the client computing device from the server computing device.

4. (Canceled)

5. (Canceled)

6. (Previously Presented) A processor-readable medium as recited in claim 1, wherein the receiving includes receiving the binary signature and the security patch from a distribution server configured to distribute to the client computing device, binary signatures that identify vulnerable files and security patches configured to fix the vulnerable files.

7. (Original) A server comprising the processor-readable medium as recited in claim 1.

8. (Currently Amended) A processor-readable medium having a tangible component and comprising processor-executable instructions configured for:

receiving a binary signature that identifies a security vulnerability in a binary file, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file located on one or more client computing devices;

receiving a security patch configured to fix the security vulnerability in the binary file; and

distributing the binary signature and the security patch to a plurality of servers to enable each respective server of the plurality of servers to:

identify, from the respective server, the particular vulnerable binary file located on a respective client computing device based on the binary signature, the client computing device being remote from the respective server; and

update, from the respective server, the particular vulnerable binary file located on the respective client computing device with the security patch;

wherein the respective server identifies the particular vulnerable binary file located on the respective client computing device by comparing the bit pattern that is associated with the security vulnerability in the particular vulnerable binary file against bit patterns of binary files located on the respective client computing device, and wherein the respective server updates the particular vulnerable binary if a bit pattern of the

particular vulnerable binary file exactly matches the bit pattern of the binary signature that is associated with the security vulnerability.

9. (Original) A processor-readable medium as recited in claim 8, wherein the distributing includes:

sending a notice to each of the plurality of servers regarding the security vulnerability and the available patch;

receiving a request to send the binary signature and the security patch; and

sending the binary signature and the security patch in response to the request.

10. (Original) A distribution server comprising the processor-readable medium as recited in claim 8.

11. (Currently Amended) A processor-readable medium having a tangible component and comprising processor-executable instructions configured for:

receiving a binary signature from a server, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file;

searching for the binary signature in binary files located on a client computer for the particular binary file;

sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature, wherein the particular binary file is found if a bit pattern of a binary file on the client computer exactly

matches the bit pattern of the binary signature that is associated with the security vulnerability;

receiving the security patch from the server; and

updating on the client computer the binary file with the security patch.

12. (Original) A client computer comprising the processor-readable medium as recited in claim 11.

13. (Currently Amended) A method comprising:

receiving a binary signature from a server and at a client computer, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file;

searching on the client computer for [[a]]the particular vulnerable file based on the binary signature;

if a vulnerable file is found on the client computer, requesting a security patch from the server, wherein the particular binary file is found if a bit pattern of a binary file on the client computer exactly matches the bit pattern of the binary signature that is associated with the security vulnerability;

receiving the security patch from the server and at the client computer in response to the request for the security patch from the client computer; and

fixing the vulnerable file with the security patch received from the server.

14. (Canceled)

15. (Canceled)

16. (Previously Presented) A method as recited in claim 13, wherein the fixing includes installing the security patch on the client computer.

17. (Original) A method as recited in claim 13, wherein the searching includes comparing the binary signature to binary information on a storage medium of the client computer.

18. (Previously Presented) A method as recited in claim 17, wherein the binary information is selected from a group comprising:

an operating system;

an application program file; and

a data file.

19. (Previously Presented) A method as recited in claim 17, wherein the storage medium is selected from a group comprising:

a hard disk;

a magnetic floppy disk;

an optical disk;

a flash memory card;

an electrically erasable programmable read-only memory; and

network-attached storage.

20. (Currently Amended) A method comprising:

receiving, at a scan/patch server, a binary signature and a security patch from a distribution server, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file;

searching, by the scan/patch server, on a client computer for [[a]]the particular vulnerable binary file associated with the binary signature; and

if [[a]]the particular vulnerable binary file is found, fixing, by the scan/patch server, the particular vulnerable binary file on the client computer with the security patch, wherein the particular vulnerable binary file is found if a bit pattern of a binary file on the client computer exactly matches the bit pattern of the binary signature that is associated with the security vulnerability.

21. (Canceled)

22. (Canceled)

23. (Currently Amended) A computer comprising:

means for receiving, at a client computer, a binary signature from a server, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file;

means for searching for [[a]]the particular vulnerable binary file located on the client computer based on the binary signature;

means for requesting, by the client computer, a security patch from the server if [[a]]the particular vulnerable binary file is found on the client computer, wherein the particular vulnerable binary file is found if a bit pattern of a binary file

on the client computer exactly matches the bit pattern of the binary signature that is associated with the security vulnerability;

means for receiving the security patch from the server at the client computer responsive to the request for the security patch; and

means for fixing the particular vulnerable binary file with the security patch received from the server.

24. (Currently Amended) A server comprising:

means for receiving, at a scan/patch server, a binary signature and a security patch from a distribution server, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file;

means for scanning, from the scan/patch server, a client computer for [[a]]the particular vulnerable binary file associated with the binary signature; and

means for fixing, from the scan/patch server, the particular vulnerable binary file on the client computer with the security patch if [[a]]the particular vulnerable binary file is found on the client computer, wherein the particular vulnerable binary file is found if a bit pattern of a binary file on the client computer exactly matches the bit pattern of the binary signature that is associated with the security vulnerability.

25. (Currently Amended) A computer having a tangible component and comprising:

binary information;

a storage medium configured to retain the binary information;

a scan module configured to receive a binary signature from a server and scan the binary information on the computer for the binary signature, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file; and

a patch module configured to request a security patch from a server and install the security patch from the server if the binary signature is found in the binary information on the computer, wherein the binary signature is found if a bit pattern of a binary file of the binary information on the client computer exactly matches the bit pattern of the binary signature that is associated with the security vulnerability.

26. (Canceled)

27. (Previously Presented) A computer as recited in claim 25, wherein the binary information is selected from a group comprising:

an operating system;

an application program file; and

a data file.

28. (Currently Amended) A computer having a tangible component and comprising:

binary files;

a storage medium configured to retain the binary files;

a binary signature; and

a security patch module configured to receive the binary signature from a server and to scan the binary files on the computer in search of the binary signature, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file;

[[a]]the particular binary file that includes the binary signature; and

a security patch;

wherein the security patch module is further configured to request the security patch from the server upon locating the binary signature within the binary file, and to apply the security patch to the binary file that includes the binary signature, wherein the binary signature is found if a bit pattern of a binary file of the binary files on the computer exactly matches the bit pattern of the binary signature that is associated with the security vulnerability.

29. (Canceled)

30. (Currently Amended) A distribution server having a tangible component and comprising:

a database; and

a distribution module configured to receive a binary signature and a security patch, store the binary signature and the security patch in the database, and distribute the binary signature and the security patch to a plurality of servers, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file located on one or more client computers, wherein the distributing of the binary signature to the plurality of servers enables each respective server of the plurality of servers to:

identify, from the respective server, the particular vulnerable binary file located on a respective client computer based on the binary signature, the client computer being remote from the respective server; and

update, from the respective server, the particular vulnerable binary file located on the respective client computer with the security patch;

wherein the respective server identifies the particular vulnerable binary file located on the respective client computer by comparing the bit pattern that is associated with the security vulnerability in the particular vulnerable binary file against bit patterns of binary files located on the respective client computer, and wherein the respective server updates the particular vulnerable binary if a bit pattern of the particular vulnerable binary file exactly matches the bit pattern of the binary signature that is associated with the security vulnerability.

31. (Original) A distribution server as recited in claim 30, wherein the distribution module is further configured to receive a request from a server for the binary signature and the security patch and to distribute the binary signature and the security patch to the server in response to the request.

32. (Currently Amended) A server having a tangible component and comprising:

a binary signature ~~associated~~ comprising a bit pattern that is associated with a security vulnerability in a particular binary file;

a security patch configured to fix the security vulnerability in the binary file;

a database embodied as a storage medium and configured to store the binary signature and the security patch; and

a scan module configured to scan, from the server, binary files on a client computer for the binary signature and to update, from the server, the binary file on the client computer with the security patch if the binary signature is found, wherein the client computer is remote from the server, wherein the binary signature is found if a bit pattern of a binary file of the binary files on the computer exactly matches the bit pattern of the binary signature that is associated with the security vulnerability.

33. (Previously Presented) A server as recited in claim 32, wherein the scan module is further configured to receive the binary signature and the security patch from a distribution server and to store the binary signature and the security patch in the database.